

IMAGE PROCESSING SYSTEM

Publication number: JP2000287065

Publication date: 2000-10-13

Inventor: MITSUI YASUHIRO

Applicant: OKI ELECTRIC IND CO LTD

Classification:

- international: G06F12/14; G06F21/24; G06T1/00; G09C5/00;
H04N1/387; G06F12/14; G06F21/00; G06T1/00;
G09C5/00; H04N1/387; (IPC1-7): H04N1/387;
G06F12/14; G06T1/00; G09C5/00

- european:

Application number: JP19990090253 19990330

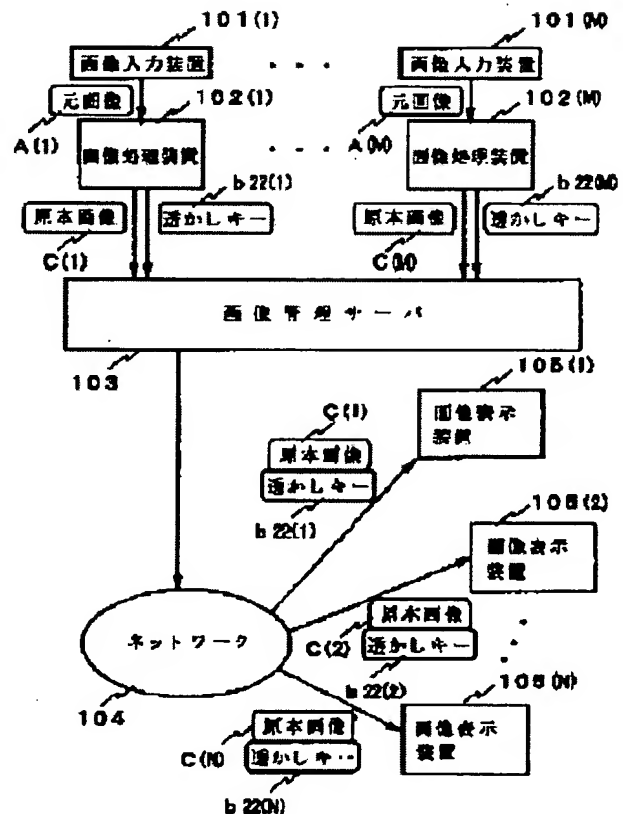
Priority number(s): JP19990090253 19990330

Report a data error here

Abstract of JP2000287065

PROBLEM TO BE SOLVED: To provide a system at a low cost, where falsification of an image file is prevented, the falsification is easily detected and only a small processing load is enough for processing the image file.

SOLUTION: This system is provided with an image processing unit 102(1) which provides an original picture C(1) resulting from imbedding electronic watermark information that can be extracted by using a watermark key, including authentication information which authenticates an image file from a legal server into an original image A(1) and provides the watermark key b 22(1) and with an image display device 105(1) which uses the watermark key served by the image processing units 102(1), extracts the electronic watermark information from the original image C(1), stores the original image C(1), whose falsification is discriminated by using the watermark key b 22(1) and the watermark key 22b(1) itself, extracts the electronic watermark information from the served original image by using the watermark key served by an image management server 103 properly serving the original image and the watermark key to a utility destination, and displays the original image C(1) whose falsification is discriminated by using the authentication information of the watermark key for a purpose of browsing.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-287065
(P2000-287065A)

(43) 公開日 平成12年10月13日 (2000. 10. 13)

(51) Int. Cl. ⁷	識別記号	F I	ターミット* (参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 5 0
G 0 6 T 1/00		G 0 9 C 5/00	5 B 0 5 7
G 0 9 C 5/00		G 0 6 F 15/62	3 3 0 A 5 C 0 7 6
		15/66	B 5 J 1 0 4

審査請求 有 請求項の数10 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平11-90253

(22) 出願日 平成11年3月30日 (1999. 3. 30)

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 三井 靖博

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

(74) 代理人 100069615

弁理士 金倉 喬二

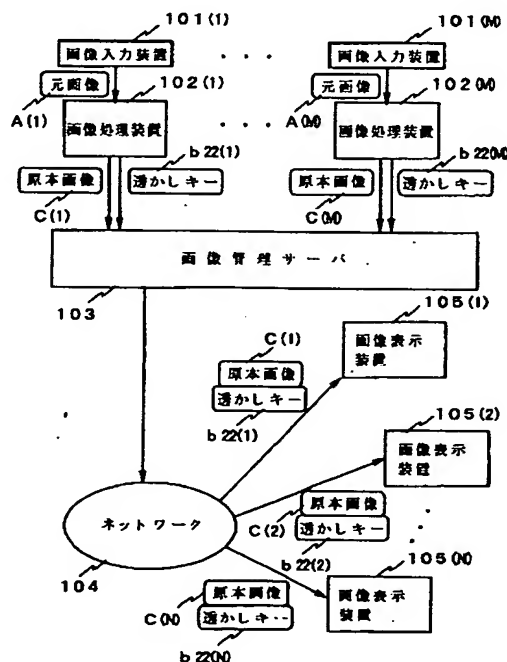
最終頁に続く

(54) 【発明の名称】 画像処理システム

(57) 【要約】 (修正有)

【課題】 画像ファイルの改竄を防止し、改竄を容易に検出し、画像ファイルの処理負荷の小さいシステムを低コストで提供する。

【解決手段】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて抽出可能な電子透かし情報を元画像 A (1) に埋め込んだ原本画像 C (1) と透かしキー b 22 (1) を提供する画像処理装置 1 0 2 (1) から提供された透かしキーを用いて、原本画像 C (1) から電子透かし情報を抽出し、改竄の有無を判断した透かしキー b 22 (1) を用いて改竄の有無を判断した原本画像 C (1) と透かしキー b 22 (1) を記憶しておく、適宜原本画像と透かしキーを利用先に提供する画像管理サーバ 1 0 3 から提供された透かしキーを用いて提供された原本画像から電子透かし情報を抽出し、透かしキーの認証情報を用いて、改竄の有無を判断した原本画像 C (1) を表示利用する画像表示装置とを備える。



【特許請求の範囲】

【請求項1】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイル及びその透かしキーを提供する画像提供装置と、

前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項2】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する機能の認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項3】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、これら画像ファイルと透かしキーを提供する画像提供装置と、

前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルと前記透かしキーを記憶しておき、適宜画像ファイルと透かしキーを利用先に提供する画像管理装置と、

この画像管理装置から提供された透かしキーを用いて前記画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項4】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像

ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、この画像ファイルを利用先に提供する画像管理装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項5】 正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、正当な提供先からの画像ファイルであることを認証する認証情報を含む付随情報を画像ファイルに付随させ、利用先から画像ファイルのアクセスがあった場合に、その画像ファイルとともに付随情報を利用先に提供する画像管理装置と、

付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項6】 請求項1において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理シ

システム。

【請求項7】 請求項3において、画像管理装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理システム。

【請求項8】 請求項3において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理システム。

【請求項9】 請求項3において、画像管理装置は、提供された透かしキーに含まれる認証情報を画像ファイルに付随する付随情報に含めて、その付随情報を画像ファイルとともに利用先に提供し、画像利用装置では、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出して改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用するようにしたことを特徴とする画像処理システム。

【請求項10】 請求項1から請求項9のいずれかにおいて、認証情報には、画像ファイルの提供先を識別する提供先識別情報又は画像ファイルを識別する画像識別情報を含むことを特徴とする画像処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像処理システムに関し、さらに詳しくは、画像の改竄防止を実現する画像処理システムに関する。なお、改竄とは、改変又は置換の2つを意味する。改変とは、画像の中身を構成するデータの値を変更することをいう。置換とは、画像を別のデータと置き換えることをいう。

【0002】

【従来の技術】従来の画像処理システムでは、画像の管理は、基本的に画像保管・処理装置におけるアクセスコントロールによって行われていた。アクセス許可を管理する方法では、画像ファイルの書き込みを禁止し読み出しのみを可能にする等の制限を行って改竄を不能にすることによって行われていた。また、暗号化による管理方法では、暗号システムと組み合わせたシステムを構成し、画像を暗号化して復号キーと暗号化画像を保管し、復号キーがなければ暗号化画像が復号できず、復号できなければ処理ができないという方法によって行われていた。

【0003】また、画像自体の暗号化とは別に、画像の改竄を検出する方法として、画像データからメッセージ・ダイジェスト、圧縮子やハッシュ値と呼ばれるデータ

の指紋とも呼ぶべき特徴的なビット・パターンを検証データとして作成して画像とは別に管理し、検証時に検証しようとする画像から検証データを作成し、その値と管理してあった検証データを比較し、異なる場合は改竄が行われているという検証方法もあった。このような検証データを作成するメッセージ・ダイジェスト関数としてもっとも広く使用されているのは、RSA社（米）のMD2、MD4、MD5といった一連のアルゴリズムである。

【0004】検証データを作成して、検証時にその値の比較によって改竄を検出するシステムでも、改竄画像から検証データを作成し、画像と検証データの両方を摩り替えることによって欺く事ができるため、検証データは必ず暗号化されて使用される。暗号システムでは、一般的に、暗号化と復号化を共通の秘密鍵（secret key）で行う「共通鍵システム」、公開されている公開鍵（public key）とその鍵の所有者以外には秘密にされている秘密鍵（private key）が使用され、一方の鍵で暗号化し他方の鍵で復号化する「公開鍵システム」が使用され、それに加えて認証を行うための電子署名が使用される。

「共通鍵システム」として代表的なものにDES（Data Encryption Standard）システム、日本電信電話株式会社のFEAL（Fast Encryption Algorithm）システム、三菱電機株式会社のMISTYシステム等があり、「公開鍵システム」として代表的なものにRSA社（米）のRSA公開鍵システムがある。

【0005】また、電子透かし技術はこれまで、日経エレクトロニクス 1997.2.24 (no. 683) に述べられているように、これまでの適用範囲のほとんどは「著作権保護」の為であり、画像品質を損なわないように、そして埋め込んだ透かしができるだけ消えないような実現方法が数多く提案されてきた。この利用方法は、知覚し難く、画像に変更を加えても消え難い電子透かしを使って、情報を埋め込み、その情報を確認することによって著作権を確認するというものであった。

【0006】電子透かしの画像検証に対する適用として、特開平10-208026号公報に述べられるように、電子透かしの一つの特徴であるステガノグラフィー（データ隠蔽）によって、スタンプ情報や元画像に埋め込み、その情報を抽出し、比較することによって、改竄を検出するという技術も提案されている。電子透かしによる情報埋め込みはさまざまな用途が提案されており、著作権情報以外にも、画像を作成した装置情報や、作成者情報、使用者情報等のさまざまな管理情報を画像内に電子透かしに埋め込むシステムが提案されている。

【0007】

【発明が解決しようとする課題】しかしながら、アクセス権だけの操作では、特権ユーザーによる改竄は防止できず、また、画像を扱うすべての装置の完全なアクセス権設定を実現することはコストのかかる作業が必要であ

った。暗号化による画像管理では、画像ファイル自体を暗号化しているために、画像を表示するたびに、復号化（及び再暗号化）の処理を行う必要があった。このため、特に、多量の画像を処理するシステムではその処理負荷が大きくなってしまいう問題点があった。また、画像がシステム内に分散した複数のマシンで利用されるシステムでは、各マシン毎に復号化（及び再暗号化）の処理が行われる為に、その処理の過程及び暗号・復号鍵の管理並びに復号された画像の管理が万全であることは記しがたく、セキュリティの甘いマシンを選んで不正を行いやすいという問題点があった。

【0008】さらに、メッセージ・ダイジェストといった検証データを用いて改竄を検出する場合でも、検証データの管理に関して、検証データの保証を行うために、検証データを管理する暗号システムが必要であり、上記の画像の暗号化と同様の問題が生じていた。

【0009】

【課題を解決するための手段】本発明の請求項1に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイル及びその透かしキーを提供する画像提供装置と、前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【0010】請求項2に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する機能の認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【0011】請求項3に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、これら画像ファイルと透かしキーを提供する画像提供装置と、前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かし

キーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルと前記透かしキーを記憶しておき、適宜画像ファイルと透かしキーを利用先に提供する画像管理装置と、この画像管理装置から提供された透かしキーを用いて前記画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【0012】請求項4に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、この画像ファイルを利用先に提供する画像管理装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【0013】請求項5に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、正当な提供先からの画像ファイルであることを認証する認証情報を含む付随情報を画像ファイルに付随させ、利用先から画像ファイルのアクセスがあった場合

に、その画像ファイルとともに付随情報を利用先に提供する画像管理装置と、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【0014】請求項6に記載の発明は、請求項1において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。請求項7に記載の発明は、請求項3において、画像管理装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。

【0015】請求項8に記載の発明は、請求項3において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。請求項9に記載の発明は、請求項3において、画像管理装置は、提供された透かしキーに含まれる認証情報を画像ファイルに付随する付随情報に含めて、その付随情報を画像ファイルとともに利用先に提供し、画像利用装置では、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出して改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用するようにしたことを構成上の特徴とする画像処理システムを提供する。

【0016】請求項10に記載の発明は、請求項1から請求項9のいずれかにおいて、認証情報には、画像ファイルの提供先を識別する提供先識別情報又は画像ファイルを識別する画像識別情報を含むことを構成上の特徴とする画像処理システムを提供する。なお、認証情報の提供先識別情報には、例えば、提供先の画像提供装置を識別する装置識別情報、提供先の画像提供装置のMACアドレス、提供先の画像提供装置が所属するシステムを識別するシステム識別情報や画像ファイルの作成者を識別する作成者識別情報がある。提供先識別情報は、データサイズ可変なハッシュ値で表すようにしてもよい。また、認証情報の画像識別情報には、例えば、画像提供装

置が画像ファイルを画像利用装置に提供する毎に繰り上がるカウント数、画像提供装置が画像ファイルを画像利用装置に提供する毎に一方方向ハッシュ関数によって更新するハッシュ値、画像提供装置が画像ファイルファイルを作成したファイル作成時間等の時間情報がある。また、請求項6又は請求項9に記載の付随情報には、例えば、画像ファイルのファイル名がある。

【0017】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態を説明する。なお、これによりこの発明が限定されるものではない。

第1の実施の形態

図1は、第1の実施の形態の画像処理システムのネットワーク構成図である。

【0018】この画像処理システムでは、画像入力装置101(1)～(M)で取り込まれた画像は、画像処理装置102(1)～(M)、画像管理サーバ103及びネットワーク104を介して画像表示装置105(1)～(N)のそれぞれで表示されるようになっている。なお、以下の説明では、画像入力装置101(1)～(M)のm番目を画像入力装置101(m)とし、画像処理装置102(1)～(M)のm番目を画像処理装置102(m)とし、画像表示装置105(1)～(N)のn番目を画像表示装置105(n)とする。

【0019】前記画像入力装置101(m)は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像A(m)として出力する。前記画像処理装置102(m)は、前記画像入力装置101(m)からの元画像A(m)をそれぞれ入力し、この元画像A(m)に電子透かしを埋め込んだ原本画像C(m)と暗号化した透かしキーb22(m)を対にして出力する機能を有する。

【0020】図2に、第1の実施の形態の画像処理装置の機能ブロック構成図を示す。この画像処理装置102(m)は、電子透かし埋め込み部21(m)と透かしキー生成部22(m)と暗号部23(m)とを有している。前記電子透かし埋め込み部21(m)は、元画像A(m)に対する改竄を検出するための電子透かしを透かしキーB22(m)を用いて元画像A(m)に埋め込んだ原本画像C(m)を出力する。前記透かしキー生成部22(m)は、前記透かしキーB22(m)を生成する。ここで、透かしキーB22(m)は、本実施の形態では、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違するようにしてもよい。

【0021】なお、元画像A(m)と原本画像C(m)と透かしキーB22(m)が簡単に手に入るとすると、いろいろな元画像A(m)とその原本画像C(m)の差分と透かしキーB22(m)の関係を調べることによって、電子透かしの埋め込み方式の解析が容易になり、原本画像C(m)の改竄や偽造の容易性を高めることになる。このため、透か

しキーB22(m)はオリジナルの状態で流通しないシステム構成が好ましく、ここでは、透かしキーB22(m)の生成にRSA等の公開鍵システムを用いて、透かしキーB22(m)のやり取りを行う場合を想定する。

【0022】図3に、第1の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部22(m)は、認証情報生成手段24(m)と透かしキー生成手段25(m)とを有している。前記認証情報生成手段24(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置102(m)を識別するための装置識別値D24a(m)と元画像A(m)を識別するための画像識別値D24b(m)とを使用する。また、認証情報生成手段24(m)には、装置識別値D24a(m)を記憶する装置識別値記憶部24a'(m)と、元画像A(m)をナンバリングするための画像識別値D24b(m)を元画像A(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ24b(m)とを備えてある。前記透かしキー生成手段25(m)は、装置識別値D24a(m)と画像識別値D24b(m)とを含む透かしキーB22(m)を生成する。例えば、装置識別値D24a(m)を「KKK F J I 1 2 3」とし、画像識別値D24b(m)を「0 1 2 3 4 5 6 7」とした場合、単純にそれぞれを繋ぎ合わせた「KKK F J I 1 2 3 0 1 2 3 4 5 6 7」を含む透かしキーB22(m)を生成する。なお、装置識別値D24a(m)としては、画像処理装置102(m)内のソフトウェアやハードウェアに設定した値を使用することができる。

【0023】図2に戻って、前記暗号部23(m)は、透かしキーB22(m)を暗号化して透かしキーb22(m)を出力する。そして、画像処理装置102(m)は、原本画像C(m)と透かしキーb22(m)とを対にして出力する。図1に戻って、前記画像管理サーバ103は、前記画像処理装置102(m)から送られてきた原本画像C(m)と透かしキーb22(m)を保存・管理するサーバであり、通常データベースやワークフローシステムとして構築され、原本画像C(m)と透かしキーb22(m)とを対にして管理する。

【0024】図4に、第1の実施の形態の画像管理サーバの機能ブロック構成図を示す。この画像管理サーバ103は、電子透かし検証部31と、認証情報・検出検証部33と、認証情報生成手段34(1)～(M)（以下、m番目を認証情報生成手段34(m)という。）と、復号部36と、記憶制御部37と、暗号部38とを有している。前記電子透かし検証部31は、画像処理装置102(m)から提供された原本画像C(m)を提供された透かしキーB22(m)を用いて電子透かしが抽出できるか否かを検証する。透かしキーB22(m)が正当なものである場

合、原本画像C(m)から電子透かしが抽出できても改竄が検出されれば改竄が行われているということが分かり、抽出できなければ原本画像C(m)が置換されていることが分かる。前記認証情報・検出検証部33は、透かしキーB22(m)から前記装置識別値D24a(m)及び前記画像識別値D24b(m)を抽出し、各認証情報生成手段34(m)で生成される装置識別値D34a(1)～(M)（以下、m番目を装置識別値D34a(m)という。）と画像識別値D34b(1)～(M)（以下、m番目を画像識別値D34b(m)という。）と比較を行うことによって、提供された透かしキーB22(m)が正当なものであるかどうかを検証する。前記認証情報生成手段34(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置102(m)を識別するための前記装置識別値D24a(m)と同一の装置識別値D34a(m)と、元画像A(m)を識別するための前記画像識別値D24b(m)と同一の画像識別値D34b(m)とを使用する。また、前記認証情報生成手段34(m)には、装置識別値D34a(m)を記憶する装置識別値記憶部34a(m)と、元画像A(m)をナンバリングするための画像識別値D34b(m)を原本画像C(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ34b(m)とを備えてある。なお、装置識別値D34a(m)の装置識別値記憶部34a(m)への記憶や画像カウンタ34b(m)のセットは、システム運用開始時又は運用中に予め行っておく。

【0025】前記復号部36は、画像処理装置102(m)から送られてきた暗号化された透かしキーb22(m)を元の透かしキーB22(m)に復号する。前記記憶制御部37は、原本画像C(m)と透かしキーB22(m)とを対にして管理する。前記暗号部38は、前記画像表示装置105(n)毎に応じて透かしキーB22(m)を暗号化した透かしキーb22(n)を生成する。そして、画像管理サーバ103は、原本画像C(m)とともに透かしキーb22(n)をそれぞれ対にして、各画像表示装置105(n)に送る（図1参照）。なお、ここでは、画像処理装置102(m)で処理された原本画像C(m)が、画像管理サーバ103を介して画像表示装置105(n)まで送られ表示される場合は、画像処理装置102(m)での画像処理回数と画像表示装置105(n)での表示回数が同じであることを想定する。この想定は、以下の各実施の形態でも同様とする。

【0026】図1に戻って、前記ネットワーク104は、例えば、LANやWAN等で構築されるネットワークである。前記画像表示装置105(n)は、原本画像C(m)を表示利用する装置である。図5に、第1の実施の形態の画像表示装置の機能ブロック構成図を示す。この画像表示装置105(n)は、電子透かし検証部51(n)

と、認証情報抽出・検証部53(n)と、認証情報生成手段54(1)～(M)（以下、m番目を認証情報生成手段54(m)という。）と、復号部56(n)と、表示制御部59(n)とを有している。前記電子透かし検証部51(n)は、画像管理サーバ103から提供された原本画像C(m)を提供された透かしキーB22(m)を用いて電子透かしが抽出できるか否かを検証する。透かしキーB22(m)が正当なものである場合、原本画像C(m)から電子透かしが抽出できても改竄が検出されれば改竄が行われているということが分かり、抽出できなければ原本画像C(m)が置換されていることが分かる。前記認証情報・検出検証部53(n)は、透かしキーB22(m)から前記装置識別値D24a(m)及び前記画像識別値D24b(m)を抽出し、認証情報生成手段54(n)で生成される装置識別値D54a(m)と画像識別値D54b(m)と比較を行うことによって、提供された透かしキーB22(m)が正当なものであるかどうかを検証する。前記認証情報生成手段54(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置102(m)を識別するための前記装置識別値D24a(m)と同一の装置識別値D54a(m)と元画像A(m)を識別するための前記画像識別値D24b(m)と同一の画像識別値D54b(m)とを使用する。また、前記認証情報生成手段54(m)には、装置識別値D54a(m)を記憶する装置識別値記憶部54a(m)と、元画像A(m)が送られて来た順番をナンバリングするための画像識別値D54b(m)を原本画像C(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ54b(m)とを備えている。なお、装置識別値D54a(m)の装置識別値記憶部54a(m)への記憶や画像カウンタ54b(m)のセットは、システム運用開始時又は運用中に予め行っておく。

【0027】前記復号部56(n)は、画像管理サーバ103から送られてきた暗号化された透かしキーb22(n)を元の透かしキーB22(m)に復号する。前記表示制御部59(n)は、提供された原本画像C(m)を図示しないCRT等の表示部に表示させる。次に、上記構成の画像処理システムの画像処理の流れを説明する。図1～図5を適宜参照するものとする。

【0028】まず、画像入力装置101(m)によって取り込まれた電子データ化した元画像A(m)は、画像処理装置102(m)に入力される。次に、画像処理装置102(m)では、透かしキー生成部22(m)で電子透かしの埋め込みのための透かしキーB22(m)を生成し、その透かしキーB22(m)を使用して電子透かし埋め込み部21(m)で電子透かしを埋め込んだ原本画像C(m)を生成する。また、画像処理装置102(m)では、暗号部23(m)が、画像管理サーバ103の公開鍵を使用して生成した透かしキーB22(m)を透かしキーb22(m)に暗号化

する。そして、画像処理装置102(m)は、原本画像C(m)と透かしキーb22(m)とを対にして画像管理サーバ103に送る。

【0029】次に、画像管理サーバ103では、復号部36が送られてきた透かしキーb22(m)を画像管理サーバ103の秘密鍵を用いて復号し、電子透かし検証部31が復号された透かしキーB22(m)を使用して原本画像C(m)の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m)の改竄が行われていないということの確認を行う。また、画像管理サーバ103では、認証情報・検出検証部33が、復号された透かしキーB22(m)から装置識別値D24a(m)及び画像識別値D24b(m)を分離し、認証情報生成手段34(m)によって生成される装置識別値D34a(m)及び画像識別値D34b(m)のそれぞれと比較する。この比較の結果、装置識別値D24a(m)と装置識別値D34a(m)とが一致するとともに画像識別値D24b(m)と画像識別値D34b(m)とが一致した場合には、提供された透かしキーB22(m)が正当な提供者から提供された正当なものであると判断する。なお、両方とも一致しない場合や一方が一致しない場合は、正当な提供先からの透かしキーB22(m)が改竄された不正なものであると判断する。さらに、画像管理サーバ103では、前記記憶制御部37が改竄の行われていない原本画像C(m)と透かしキーB22(m)とを対にして管理する。ここで、画像管理サーバ103は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像C(m)は正当なものでないため、改竄検出の警告を表示等により報知して、その原本画像C(m)の表示を行わないことで、改竄画像による不正を防止できる。そして、前記画像表示装置105(n)から原本画像C(m)の転送を要求されたり自動的に転送する場合には、画像管理サーバ103は前記暗号部38で、前記画像表示装置105(n)毎に応じて透かしキーB22(m)を暗号化した透かしキーb22(n)を生成し、原本画像C(m)とともにその透かしキーb22(n)をそれぞれ対にして各画像表示装置105(n)に送る。

【0030】各画像表示装置105(n)では、復号部56(n)が送られてきた透かしキーb22(n)を画像表示装置105(n)の秘密鍵を用いて復号し、電子透かし検証部51(n)が復号された透かしキーB22(m)を使用して原本画像C(m)の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m)の改竄が行われていないということの確認を行う。また、画像表示装置105(n)では、認証情報・検出検証部53(m)が、復号された透かしキーB22(m)から装置識別値D24a(m)及び画像識別値D24b(m)を分離し、認証情報生成手段54(m)によって生成される装置識別値D54a(m)及び画像識別値D54b(m)のそれぞれと比較する。この比較の結果、装置識別値D24a(m)と装置識別値D54a(m)とが一致するとともに画像識別値D24b(m)と画像識別値D54b(m)とが

一致した場合には、提供された透かしキーB22(m)が正当な提供者から提供された正当なものであると判断する。なお、両方とも一致しない場合や一方が一致しない場合は、正当な提供先からの透かしキーB22(m)が改竄された不正なものであると判断する。さらに、画像管理サーバ103では、提供された原本画像C(m)が改竄されていないことが判明すれば、前記表示制御部59(n)は、原本画像C(m)を図示しないCRT等の表示部に表示させる。

【0031】したがって、画像表示装置105(n)は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像C(m)は正当なものでないため、改竄検出の警告を表示等により報知して、その原本画像C(m)の表示を行わないことで、改竄画像による不正を防止できる。上記第1の実施の形態によれば、画像を利用する際に画像表示しか行わない画像処理装置において、改竄検出可能な電子透かしを埋め込んだ原本画像と、認証情報を含む透かしキーとを提供し、提供先で透かしキーを使用して原本画像から電子透かしを抽出するようにしたため、原本画像の改竄を検出することが可能になる。また、提供先において、認証情報を含む透かしキーから認証情報を取り出し、また、透かしキーが正当であれば取り出した認証情報と同一の認証情報を生成して、互いに比較することで透かしキーの正当性を認証することができる。このため、提供された透かしキーを用いて提供された原本画像から電子透かしが抽出できない場合に、透かしキーの正当性が確認されていなければ、原本画像自体に改竄が行われたのか又は透かしキーに改竄が行われたのかを判別することができないが、本実施の形態のように透かしキーの正当性が確認されれば、原本画像に何らかの改竄があることを判別することができるようになる。したがって、本実施の形態では、他の認証機構を導入する必要がなく、画像処理装置の成りすましや、画像の摩り替えに対するセキュリティを向上することができる。

【0032】また、本実施の形態では、従来のように画像を暗号化して管理し、復号しなければ表示できない暗号システムに比べると、画像を画像データとして管理できるため画像データ管理部分は通常の画像処理システムと同等に構成でき、一度原本画像を作成した後は、特に、オリジナルの元画像データは作成されることがない場合には、画像の改変を高度に防ぐことが可能となる。

【0033】なお、上記第1の実施の形態では、透かしキーを暗号化して転送を行う例を示したが、透かしキーは、電子透かしを埋め込む際にも使用するが、電子透かしを埋め込んだ原本画像作成後は、電子透かしを抽出し検証するためにだけ使用するキーであり、暗号システムにおける復号鍵とは異なり、元画像に戻す為の鍵ではないため、その管理を復号鍵に比べて緩いものにできるという特徴もある。画像入力装置と画像処理装置と画像管

理サーバが、いわゆる対タンパ性を持つ一体された高いセキュリティな装置である場合、例えば、外部からハッキングされない、内部を見ることができない又はシステム等を破壊されない装置である場合、元画像データが搾取される可能性が低いため、透かしキーの機密性を緩めることが可能であり、オリジナルのまま移動させても問題は少ない。ただし、透かしキーによる原本画像の検証が成立したとしても、原本画像と透かしキーの両方を偽造したものと摩り替えることによって電子透かしの検証を成立させることもできる。原本画像又は透かしキーだけが不当なものに摩り替えられたとしても、検証が成立せずに露見する。原本画像が正当なもので、画像の摩り替えも改変も行われていない、つまり改竄されていないことを示す為には、まず、透かしキーが正当なものであり、その透かしキーを用いて原本画像から電子透かしが抽出され、その後、電子透かしの検証によって画像の改竄が検出されないことが必要である。

【0034】電子透かしの検証を成立させる偽造した原本画像と透かしキーの作成の可能な方法の一つとして画像処理装置を不正利用し、その画像処理装置を用いて作成した原本画像・透かしキーと摩り替える方法がある。処理がソフトウェアで行われるのであれば、そのソフトウェアを盗み出し不正利用することが可能である。しかし、本実施の形態では、この画像処理装置がセキュリティの要であり、これが盗まれなければ問題の起きる可能性は非常に低くなる。また、透かしキー生成部と電子透かし埋め込み部をハードウェアにインプリメントし、処理を隠蔽し、盗まれにくくすることであるが、コスト及び実現の容易性を考えると、ソフトウェアにおけるインプリメントの処理における対策も必要である。このため、本実施の形態のように、認証情報を含む透かしキーを使用することで、原本画像及び透かしキーを送ってきた画像処理装置が正当なものであるという認証を行うことができるようになる。

【0035】第2の実施の形態

以下、上記第1の実施の形態との相違点を説明する。本第2の実施の形態は、上記第1の実施の形態と比較して透かしキーに含まれる認証情報の内の画像識別値を画像カウンタのカウント数ではなく、画像ファイル毎にラベリングするハッシュ値とした。なお、ハッシュ値とするのは、どのような認証情報に対しても行うことが可能であり、それらの説明は省略する。また、画像処理システムのネットワークは、上記第1の実施の形態の場合を想定し、その説明は省略する。

【0036】図6に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部22(m)は、認証情報生成手段24(m)と透かしキー生成手段25(m)とを有している。前記認証情報生成手段24(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報

は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値D24a(m)と、元画像A(m)を識別するための画像識別値D24c(m)とを使用する。この画像識別値D24c(m)が、本第2の実施の形態では、ハッシュ値としたのである。このハッシュ値は、一方向ハッシュ関数により生成される。一方向ハッシュ関数としては、例えば、RSA社(米)のMD4、MD5やSHA(Secure Hash Algorithm)等がある。

【0037】このため、前記認証情報生成手段24(m)には、装置識別値D24a(m)を記憶する装置識別値記憶部24a(m)と、元画像A(m)をナンバリングするための画像識別値D24c(m)を元画像A(m)の処理毎にハッシュ値を生成するハッシュ値生成部24c(m)とを備えてある。前記透かしキー生成手段25(m)は、装置識別値D24a(m)及びハッシュ値としての画像識別値D24c(m)を含む透かしキーB22(m)を生成する。なお、ハッシュ値を生成するには、初期値c(m)が必要であり、この初期値c(m)は、システム運用開始時等に予め設定しておく。そして、運用が開始されると、ハッシュ値生成部24c(m)は初期値c(m)からハッシュ値を生成し、その後はフィードバックされる一つ前の画像に対して生成されたハッシュ値から現画像のハッシュ値を作成し、透かしキー生成手段25(m)はその値から透かしキーB22(m)を生成することになる。

【0038】なお、上述した前記透かしキー生成部22(m)の認証情報生成手段24(m)は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。また、画像管理サーバや画像入力装置にも、一方向ハッシュ関数の初期値は、システム運用開始時に予め設定しておけばよいが、初期値として画像処理装置の装置識別値を使用してもよい。この場合、画像管理サーバや画像表示装置では、装置識別値を入力するだけで初期値も設定することができる。また、画像管理サーバと画像表示装置との間のやり取りで透かしキーを替えるような場合には、画像処理装置と画像管理サーバとの間で使用するハッシュ値の設定は画像管理サーバのみ装置識別値の入力を行えばよいことになる。

【0039】本第2の実施の形態では、ハッシュ値により生成した認証情報を含む透かしキーとしたため、一方向ハッシュ関数の特徴により初期値と利用関数と現適用回数がわからなければ認証情報の作成が非常に困難であり、上記第1の実施の形態のようにカウンタ利用の場合に比べ透かしキーの偽造は困難となり、セキュリティが高くなる効果が得られる。また、生成されるハッシュ値は、ハッシュ値サイズは固定であるという特徴があるため、透かしキーのサイズに制限があるような電子透かし

を使用した場合には制限内に収めるのに有用である。

【0040】第3の実施の形態

以下、上記第1の実施の形態との相違点を説明する。本第3の実施の形態は、上記第1の実施の形態と比較して透かしキーに含まれる認証情報の内の画像識別値を画像カウンタのカウント数ではなく、画像ファイルを作成したファイル作成時間とした。

【0041】図7に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部22(m)は、認証情報生成手段24(m)と透かしキー生成手段25(m)とを有している。前記認証情報生成手段24(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値D24a(m)と、元画像A(m)を識別するための画像識別値D24d(m)とを使用する。この画像識別値D24d(m)が、本第3の実施の形態では、ファイル作成時間としたのである。

【0042】このため、前記認証情報生成手段24(m)には、装置識別値D24a(m)を記憶する装置識別値記憶部24a(m)と、元画像A(m)をナンバリングするための画像識別値D24d(m)を元画像A(m)の処理毎のファイル作成時間を刻むタイマ24d(m)とを備えてある。なお、ファイル作成時間はほぼすべてのファイルシステムにおいて画像ファイルと共に保持されるため、通常は、前記タイマ24dは特別に設ける必要がない。前記透かしキー生成手段25(m)は、装置識別値D24a(m)及びファイル作成時間としての画像識別値D24d(m)を含む透かしキーB22(m)を生成する。

【0043】図8に、画像管理サーバの認証情報生成手段の機能ブロック構成図を示す。この認証情報生成手段34(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値D34a(m)と、元画像A(m)を識別するための画像識別値D34d(m)とを使用する。この画像識別値D34d(m)が、本第3の実施の形態では、ファイル作成時間としたのである。

【0044】このため、前記認証情報生成手段34(m)には、装置識別値D34a(m)を記憶する装置識別値記憶部34a(m)と、元画像A(m)をナンバリングするための画像識別値D34d(m)を元画像A(m)の処理毎のファイル作成時間を記憶するタイムスタンプ記憶部34d(m)とを備えてある。なお、ファイル作成時間はほぼすべてのファイルシステムにおいて、ファイル作成時間が画像ファイルに付随する付随情報として画像ファイルとともに

転送される。このため、タイムスタンプ記憶部 34d(m) は、通常は設ける必要がない。

【0045】なお、上述した前記認証情報生成手段 34(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。本第 3 の実施の形態では、画像識別値としてファイル作成時間を使用し、このファイル作成時間により生成した認証情報を含む透かしキーとしたため、上記第 1 の実施の形態に比べ、画像カウンタが不用になる。なお、通常のファイルシステムのように、ファイル作成時間を誰にでも確認可能な状態で転送すると、セキュリティが低くなるため、暗号化して転送するのが好ましい。

【0046】第 4 の実施の形態

以下、上記第 1 の実施の形態との相違点を説明する。本第 4 の実施の形態は、上記第 1 の実施の形態と比較して透かしキーに含まれる認証情報に元画像の作成者を識別する作成者情報を追加したものである。また、画像処理システムのネットワークは、上記第 1 の実施の形態の場合を想定し、その説明は省略する。

【0047】図 9 に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部 22(m) は、認証情報生成手段 24(m) と透かしキー生成手段 25(m) とを有している。前記認証情報生成手段 24(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。また、透かしキー生成部 25(m) には、元画像 A(m) の作成者を認証する作成者認証装置 24e(m) が接続している。この作成者認証装置 24e(m) は、画像処理装置の外部の設けても、内部に設けてもよい。本実施の形態の認証情報には、提供先を識別するための認証情報には、前記提供先識別情報と前記画像識別情報と前記作成者情報がある。ここでは、提供先である画像処理装置を識別するための装置識別値 D24a(m) と、元画像 A(m) を識別するための画像識別値 D24b(m) と、元画像の作成者を識別する作成者情報 D24e(m) を使用する。この作成者情報 D24e(m) が、本第 3 の実施の形態で追加したものである。この作成者情報としては、例えば、作成者 ID、作成者氏名、指紋情報、アイリス情報、顔画像データ等がある。このため、前記画像認証装置 24e(m) は、パスワード認証、指紋認証、アイリス認証、顔写真認証等を行う機能を有する必要がある。なお、作成者情報 D24e(m) は、システム運用開始時又は運用中に予め設定しておけばよい。

【0048】また、前記認証情報生成手段 24(m) には装置識別値記憶部 24a(m) と画像カウンタ 24b(m) とを備えてあり、前記透かしキー生成手段 25(m) は、装置識別値 D24a(m)、画像識別値 D24b(m) 及び作成者情報 D24e(m) を含む透かしキー B22(m) を生成する。なお、上述した前記透かしキー生成部 22(m) の認証情報

生成手段 24(m) に接続する作成者認証装置 24e(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。また、画像管理サーバや画像入力装置にも、作成者情報 D24e(m) の設定をシステム運用開始時に予め設定しておけばよい。

【0049】本第 4 の実施の形態によれば、画像取り込み時の偽造防止や改竄発覚時の作成者特定のために画像処理装置において画像処理を行う際に、作成者認証を行い、透かしキー作成情報として作成者情報を含めたため、その原本画像の作成者の特定を行いやすくなる。したがって、偽造判明後の作成者の追跡を行いやすくなり、また、画像処理装置を利用して不正な原本画像が作成された場合、作成者の特定を行う追跡調査を容易にし、偽造防止・偽造抑止の効果を大幅に向上させることができる。

【0050】つまり、一般的には、画像処理装置の操作時に認証を行い、改竄発覚時にはその認証ログおよび画像処理ログを解析することによって、作成者の特定が行えるシステムでは、ログの改竄等によって作成者特定作業を妨げることが可能であるが、さらに、本実施の形態では、透かしキーに作成者情報を含めたことにより、電子透かしと透かしキーの検証の結果、改竄が検出された場合、改竄者の特定を行うことができるようになる。改竄者といえども改竄者自身の作成者情報を用いない限り、電子透かしを埋め込むことができないからである。

【0051】また、複数の許可者がいる場合は、透かしキーの生成を許可者数分行い、検証できた透かしキーを使用するのが一番容易である。このため、作成許可者 ID 等と許可者情報のテーブルを画像管理サーバと画像表示装置に登録しておき、作成者情報そのものでなく、作成許可者 ID 等の情報を通信によって受け渡し、作成許可者 ID から作成許可者情報を検索し、それを透かしキー作成に使用するようにしてもよい。この場合、作成者情報そのものを暗号化して通信によって受け渡すのが好ましい。

【0052】さらに、システムが大きい場合は、作成許可者の管理を容易にするために画像処理の作成許可者を登録しておくデータベースである作成許可者データベース装置をシステム内に準備しておくのが好ましい。これにより、作成許可者の管理が集中して行え、また、管理場所が一つであるため作成者情報のセキュリティ保持が容易に行える。

【0053】なお、作成者情報としては、作成者認証装置やセキュリティ上の考慮からさまざまなタイプのあり、その中でも、例えば、顔写真画像のように大きなサイズのデータの場合に、透かしキーとして使用できるデータサイズに制限があるときには、一方方向ハッシュ関数を使用して、大きなデータを固定サイズのハッシュ値に

変換し、そのハッシュ値を作成者情報に追加した認証情報を含む透かしキーを使用するのが好ましい。

【0054】第5の実施の形態

以下、上記第1の実施の形態との相違点を説明する。本第5の実施の形態は、上記第1の実施の形態と比較して透かしキーに含まれる認証情報の内の装置を特定する装置識別値ではなく、LANが敷設してある場合のMACアドレスを装置識別に使用するようにした。また、画像処理システムのネットワークは、上記第1の実施の形態の場合を想定し、その説明は省略するが、ここでは、特に、画像処理装置と画像管理サーバがLANで接続されており、LANボードが組み込まれている場合を想定する。

【0055】図10に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部22(m)は、認証情報生成手段24(m)と透かしキー生成手段25(m)とを有している。前記認証情報生成手段24(m)は、正当な提供先からの画像ファイルであることを認証する認証情報の内で元画像A(m)を識別するための画像識別値D24b(m)を生成する機能を有する。また、透かしキー生成部25(m)には、提供先である画像処理装置を識別するための装置識別値としての自らのMACアドレスD24f(m)を検出するMACアドレス検出部24f(m)が接続している。このMACアドレス検出部24f(m)は、画像処理装置の外部に設けても、内部に設けてもよい。MACアドレスD24f(m)は、画像処理装置に固有の番号である。また、前記認証情報生成手段24(m)には、装置識別値D24a(m)を記憶する装置識別値記憶部24aを備えてある。前記透かしキー生成手段25(m)は、装置識別値としてのMACアドレスD24f(m)及び画像識別値D24b(m)を含む透かしキーB22(m)を生成する。

【0056】なお、本実施の形態では、画像管理サーバや画像表示装置には、予め画像処理装置のMACアドレスを記憶する記憶部を設ければ、上記第1の実施の形態と同様に、透かしキーが正当なものか否かを判断することができるため、画像管理サーバ及び画像表示装置の説明は省略する。なお、MACアドレスを使用した場合には、透かしキーを送ってきた画像処理装置のMACアドレスは画像管理サーバで認識可能なため、MACアドレスの記憶部を設けなくとも、そのMACアドレスと透かしキーから分離した装置識別値の比較を行うことが可能である。この場合は、下記第7の実施の形態で説明する。

【0057】本第5の実施の形態では、装置識別値としてMACアドレスを使用した認証情報を含む透かしキーとしたため、装置識別値を新たに設定する必要がない。

第6の実施の形態

以下、上記第1の実施の形態との相違点を説明する。本第6の実施の形態は、上記第1の実施の形態と比較して

透かしキーに含まれる認証情報に画像処理装置が所属するシステムを識別するシステム情報を追加したものである。また、画像処理システムのネットワークは、上記第1の実施の形態の場合を想定し、その説明は省略する。

【0058】図11に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部22(m)は、認証情報生成手段24(m)と透かしキー生成手段25(m)とを有している。前記認証情報生成手段24(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。また、透かしキー生成部25(m)には、画像処理装置が所属するシステムを識別するシステム情報D24g(m)を記憶したシステム情報記憶部24g(m)が接続している。このシステム情報記憶部24g(m)は、画像処理装置の外部に設けても、内部に設けてもよい。本実施の形態の認証情報には、前記提供先識別情報と前記画像識別情報と前記システム情報がある。ここでは、提供先である画像処理装置を識別するための装置識別値D24a(m)と、元画像A(m)を識別するための画像識別値D24b(m)と、システム情報D24g(m)を使用する。このシステム情報D24g(m)が、本第6の実施の形態で追加したものであり、システム運用開始時又は運用中に予め設定しておけばよい。なお、画像処理装置が多数の場合には、手間や管理が負担となるため、ソフトウェアのコンパイル時に指定して、ソフトウェア中に取り出し難いように埋め込む方が簡単で安全である。

【0059】また、前記認証情報生成手段24(m)には、装置識別値記憶部24a(m)と画像カウンタ24b(m)とを備えてある。前記透かしキー生成手段25(m)は、装置識別値D24a(m)、画像識別値D24b(m)及びシステム情報D24g(m)を含む透かしキーB22(m)を生成する。なお、上述した前記透かしキー生成部22(m)の認証情報生成手段24(m)に接続するシステム情報記憶部24g(m)は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。

【0060】本第6の実施の形態によれば、画像ファイルに電子透かしを埋め込む透かしキーにシステムを識別するシステム情報を含めたため、システム外からの不正行為防止が可能となる。たとえば、本実施の形態によると、同じシステム内での不正に対しての確認や対策だけでなく、同じ方式によって作成された他のシステムの装置やツールを利用した偽造を判明させるのが容易になる。つまり、同じシステム方式の他のシステムの画像処理装置やソフトウェア処理としてインプリメントされている場合に、たとえば、画像処理ソフトウェアが盗まれたりして不正が行われたときでも、システム毎にシステム情報が異なる為に偽造された原本画像と透かしキーを検証時に発見することができるため、不正利用を防ぐこ

とができるようになる。

【0061】第7の実施の形態

図12は、第7の実施の形態の画像処理システムのネットワーク構成図である。この画像処理システムでは、画像入力装置101(1)～(M)で取り込まれた画像は、画像処理装置106(1)～(M)、画像管理サーバ107及びネットワーク104を介して画像表示装置108(1)～(N)のそれぞれで表示されるようになっている。なお、以下の説明では、画像入力装置101(1)～(M)のm番目を画像入力装置101(m)とし、画像処理装置106(1)～(M)のm番目を画像処理装置106(m)とし、画像表示装置108(1)～(N)のn番目を画像表示装置108(n)とする。ここでは、特に、画像処理装置106(m)と画像管理サーバ107が図示しないLANで接続されており、LANボードが組み込まれている場合を想定する。

【0062】前記画像入力装置101(m)は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像A(m)として出力する。前記画像処理装置106(m)は、前記画像入力装置101(m)からの元画像A(m)をそれぞれ入力し、この元画像A(m)に電子透かしを埋め込んだ原本画像C(m)を出力する機能を有する。

【0063】図13に、第7の実施の形態の画像処理装置の機能ブロック構成図を示す。この画像処理装置106(m)は、電子透かし埋め込み部61(m)と透かしキー生成部62(m)とMACアドレス検出部64d(m)とを有している。前記電子透かし埋め込み部61(m)は、元画像A(m)に対する改竄を検出するための電子透かしを透かしキーB62(m)を用いて元画像A(m)に埋め込んだ原本画像C(m)を出力する。前記透かしキー生成部62(m)は、前記透かしキーB22(m)を生成する。ここで、透かしキーB62(m)は、本実施の形態では、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違するようにしてもよい。

【0064】なお、上記第1の実施の形態の説明と同様に、本第7の実施の形態でも透かしキーB62(m)の生成にRSA等の公開鍵システムを用いて、透かしキーB62(m)のやり取りを行う場合を想定する。図14に、第7の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部62(m)は、認証情報生成手段64(m)と透かしキー生成手段65(m)とを有している。前記認証情報生成手段64(m)は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置106(m)を識別するためのMACアドレスD64d(m)と元画像A(m)を識別する

ための画像識別値D64b(m)とを使用する。また、認証情報生成手段64(m)には、元画像A(m)をナンバリングするための画像識別値D64b(m)を元画像A(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ64b(m)とを備えてある。前記透かしキー生成手段65(m)は、MACアドレスD64d(m)と画像識別値D64b(m)とを含む透かしキーB62(m)を生成する。例えば、MACアドレスD64d(m)を「00:AB:20:CD:40:EF」とし、画像識別値D64b(m)を「0x00000001」とした場合、それぞれを組み合わせた「0x00AB20CD40EF00000001」を含む透かしキーB62(m)を生成する。なお、上記第4の実施の形態で説明した作成者情報D24e(m)を含めた透かしキーB62(m)の場合には、例えば、MACアドレスD64d(m)を「00:AB:20:CD:40:EF」とし、画像識別値D64b(m)を「0x01234567」とし、作成者情報D24e(m)の16進データを「0x89AB01BE9859」とした場合、それぞれを組み合わせた「0x00AB20CD40EF0123456789AB01BE9859」を含む透かしキーB62(m)を生成する。作成者情報D24e(m)の16進データが長い場合には、例えば、「0xFF0122CFAA234C5688FE0100EF0100EFA289EF」のハッシュ値にして、「0x00AB20CD40EF0123456789AB01BE9859FF0122CFAA234C5688FE0100EF0100EFA289EF」を含む透かしキーB62(m)を生成する。

【0065】図13に戻って、前記MACアドレス検出部64d(m)は、画像処理装置106(m)自体のMACアドレスD64d(m)を検出する。そして、画像処理装置106(m)は、原本画像C(m)を出力する。図12に戻って、前記画像管理サーバ107は、前記画像処理装置106(m)から送られてきた原本画像C(m)を保存・管理するサーバであり、通常のデータベースやワークフローシステムとして構築される。

【0066】図15に、第7の実施の形態の画像管理サーバの機能ブロック構成図を示す。この画像管理サーバ107は、MACアドレス検出部70と、電子透かし検証部71と、透かしキー生成部72と、この透かしキー生成部72内に備える認証情報生成手段74(1)～(M)（以下、m番目を認証情報生成手段74(m)という。）及び透かしキー生成手段75と、記憶制御部77と、ファイル名作成部90と、MACアドレスデータベース91とを有している。前記MACアドレス検出部70は、提供先である画像処理装置106(m)を識別するための前記画像処理装置106(m)のMACアドレスD64d(m)を検出する。前記電子透かし検証部71は、画像処理装置106(m)から提供された原本画像C(m)を生成された透かしキーB72(m)を用いて電子透かしが抽出できるか否かを検証する。原本画像C(m)から電子透かshiを抽出できなければ原本画像C(m)に改竄が行われているということが分かり、抽出できれば改竄が行われていないということが分かる。前記透かしキー生成部72は、透かしキーB72(m)を生成する機能を有し、前記認証情報

生成手段74(m)と透かしキー生成手段75とを備えている。前記認証情報生成手段74(m)は、元画像A(m)をナンバリングするための画像識別値D74b(1)~(M)

(以下、m番目を画像識別値D74b(m)という。)を原本画像C(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ74b(m)とを備えてある。なお、画像カウンタ74b(m)のセットは、システム運用開始時又は運用中に予め行っておく。前記透かしキー生成手段75は、前記MACアドレス検出部70が検出したMACアドレスD64d(m)と画像識別値D74b(m)とを含む透かしキーB72(m)を生成する。

【0067】前記記憶制御部77は、原本画像C(m)とこれに付随する情報としてのファイル名F(m)を管理する。前記ファイル名作成部90は、画像処理装置106(m)のMACアドレスD64d(m)に基づくファイル名F(m)を作成する。前記MACアドレスデータベース91は、MACアドレスD64d(m)に基づくファイル名F(m)の定義テーブルを格納してある。したがって、ファイル名作成部90は、MACアドレスD64d(m)に基づくファイル名F(m)をMACアドレスデータベース91から得ることができる。なお、ファイル名作成部90が一定の定義式に基づきその都度ファイル名F(m)を作成するようにしてもよい。そして、画像管理サーバ107は、原本画像C(m)とともにファイル名F(m)を付随させて、各画像表示装置108(n)に送る(図12参照)。

【0068】図12に戻って、前記ネットワーク104は、例えば、LANやWAN等で構築されるネットワークである。前記画像表示装置108(n)は、原本画像C(m)を表示利用する装置である。図16に、第7の実施の形態の画像表示装置の機能ブロック構成図を示す。この画像表示装置108(n)は、電子透かし検証部81(n)と、透かしキー生成部82(n)と、この透かしキー生成部82(n)内に備える認証情報生成手段84(1)~(M)(以下、m番目を認証情報生成手段74(m)という。)及び透かしキー生成手段85(n)と、表示制御部89(n)と、MACアドレスデータベース91(n)と、ファイル名処理部92(n)とを有している。前記電子透かし検証部81(n)は、画像管理サーバ107から提供された原本画像C(m)を生成した透かしキーB72(m)を用いて電子透かしが抽出できるか否かを検証する。原本画像C(m)から電子透かしを抽出できなければ原本画像C(m)に改竄が行われているということが分かり、抽出できれば改竄が行われていないということが分かる。前記透かしキー生成部82(n)は、透かしキーB72(m)を生成する機能を有し、前記認証情報生成手段84(m)と透かしキー生成手段85(n)とを備えている。前記認証情報生成手段84(m)は、元画像A(m)をナンバリングするための画像識別値D74b(1)~(M)(以下、m番目を画像識別値D74b(m)という。)を原本画像C(m)の処理毎に繰り上がるカウント数として出力する画像カウンタ

84b(m)とを備えてある。なお、画像カウンタ84b(m)のセットは、システム運用開始時又は運用中に予め行っておく。前記透かしキー生成手段85は、前記ファイル名処理部92(n)からのMACアドレスD64d(m)と画像識別値D84b(m)とを含む透かしキーB72(m)を生成する。なお、画像識別値D84b(m)は、前記画像識別値D74b(m)と同一になるように設定してある。前記MACアドレスデータベース91(n)は、MACアドレスD64d(m)に基づくファイル名F(m)の定義テーブルを格納してある。前記ファイル名処理部92(n)は、MACアドレスデータベース91(n)を参照して、ファイル名F(m)から画像処理装置106(m)のMACアドレスD64d(m)を得る。なお、ファイル名作成部92(n)が一定の定義式に基づきその都度ファイル名F(m)からMACアドレスデータベース91(n)を参照して、画像処理装置106(m)のMACアドレスD64d(m)を得るようにしてもよい。前記表示制御部59(n)は、提供された原本画像C(m)を図示しないCRT等の表示部に表示させる。

【0069】次に、上記構成の画像処理システムの画像処理の流れを説明する。図12~図6を適宜参照するものとする。まず、画像入力装置101(m)によって取り込まれた電子データ化した元画像A(m)は、画像処理装置106(m)に入力される。次に、画像処理装置106(m)では、透かしキー生成部62(m)で電子透かしの埋め込みのための透かしキーB62(m)を生成し、その透かしキーB62(m)を使用して電子透かし埋め込み部61(m)で電子透かしの埋め込んだ原本画像C(m)を生成する。また、画像処理装置106(m)では、MACアドレス検出部64d(m)が、自らのMACアドレスD64d(m)を検出して、そのMACアドレスD64d(m)の一部又は全部を透かしキーB62(m)に含めるようになっている。そして、画像処理装置106(m)は、原本画像C(m)を画像管理サーバ107に送る。

【0070】次に、画像管理サーバ107では、MACアドレス検出部70が画像処理装置106(m)のMACアドレスD64d(m)を検出し、透かしキー生成手段75がそのMACアドレスD64d(m)を含む透かしキーB72(m)を生成し、電子透かし検証部71がその生成した透かしキーB72(m)を使用して原本画像C(m)の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m)の改竄が行われていないというの確認を行う。そして、前記画像表示装置108(n)から原本画像C(m)の転送を要求されたり自動的に転送する場合には、画像管理サーバ107は、画像処理装置106(m)のMACアドレスD64d(m)に基づいたファイル名F(m)を原本画像C(m)に付随させて各画像表示装置108(n)に送る。

【0071】各画像表示装置108(n)では、送られてきたファイル名F(m)から画像処理装置106(m)のMACアドレスD64d(m)を得て、透かしキー生成手段85

(n)がこのMACアドレスD64d(m)を含む透かしキーB72(m)を生成し、電子透かし検証部81(n)がその生成した透かしキーB72(m)を使用して原本画像C(m)の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m)の改竄が行われていないということの確認を行う。そして、前記表示制御部59(n)は、原本画像C(m)を図示しないCRT等の表示部に表示させる。

【0072】したがって、画像表示装置108(n)は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像C(m)は正当なものでないため、改竄検出の警告を表示等により報知して、その原本画像C(m)の表示を行わないことで、改竄画像による不正を防止できる。上記第7の実施の形態によれば、画像管理サーバから画像表示装置へは、認証情報に基づく付随情報を画像ファイルに付随させて受け渡すようにしたため、画像表示装置でも透かしキーを生成することが可能になる。なお、画像処理装置から画像管理サーバの場合も同様に受け渡すようにしてもよい。また、画像処理装置から画像管理サーバの場合では、LAN接続されている場合を想定したため、透かしキーの認証情報としてMACアドレスを使用すると、画像管理サーバはMACアドレスの受け取りをシステムを変更せずに、LAN上で行うことができる。

【0073】第8の実施の形態

図17は、第8の実施の形態の画像処理システムのネットワーク構成図である。この画像処理システムでは、画像入力装置101(m)で取り込まれた画像は、画像処理装置110(m)、画像管理サーバ120及びネットワーク104を介して画像表示装置130(n)のそれぞれで表示されるようになっている。なお、以下の説明では、(m)及び(n)は、上記各実施の形態で使用したのと同じの意味で使用するものとする。

【0074】前記画像入力装置101(m)は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像A(m)として出力する。前記画像処理装置110(m)は、前記画像入力装置101(m)からの元画像A(m)をそれぞれ入力し、この元画像A(m)に電子透かしを埋め込んだ原本画像H(m)を出力する機能を有する。このため、電子透かし埋め込み部112(m)と透かしキー生成部111(m)とを有している。前記電子透かし埋め込み部112(m)は、元画像A(m)に対する改竄を検出するための電子透かしを透かしキーG111(m)を用いて元画像A(m)に埋め込んだ原本画像H(m)を出力する。前記透かしキー生成部111(m)は、上記各実施の形態で説明した認証情報を含む前記透かしキーG111(m)を生成する。ここで、透かしキーG111(m)は、本実施の形態では、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違す

るようにしてもよい。なお、上記実施の形態と同様に、透かしキーG111(m)の生成にRSA等の公開鍵システムを用いて、透かしキーG111(m)のやり取りを行う場合を想定する。

【0075】前記画像管理サーバ120は、前記画像処理装置110(m)から送られてきた原本画像H(m)を保存・管理するサーバであり、通常のデータベースやワークフローシステムとして構築され、電子透かし埋め込み部122(m)と透かしキー生成部121(m)とを有している。前記電子透かし埋め込み部122(m)は、原本画像H(m)に対する改竄を検出するための電子透かしを透かしキーG121(m)を用いて抽出して検証する。前記透かしキー生成部121(m)は、前記透かしキーG111(m)と同一の前記透かしキーG121(m)を生成する。なお、透かしキー生成部121(m)内の図示しない装置識別値記憶部への記憶や図示しない画像カウンタのセット等は、システム運用開始時又は運用中に予め行っておく。

【0076】前記ネットワーク104は、例えば、LANやWAN等で構築されるネットワークである。前記画像表示装置130(n)は、原本画像C(m)を表示利用する装置であり、電子透かし埋め込み部132(n)と透かしキー生成部131(n)とを有している。前記電子透かし埋め込み部132(n)は、原本画像H(m)に対する改竄を検出するための電子透かしを透かしキーG131(m)を用いて抽出して検証する。前記透かしキー生成部131(n)は、前記透かしキーG111(m)と同一の前記透かしキーG131(m)を生成する。なお、透かしキー生成部131(n)内の図示しない装置識別値記憶部への記憶や図示しない画像カウンタのセット等は、システム運用開始時又は運用中に予め行っておく。

【0077】上述した構成では、画像管理サーバ110(m)は、透かしキー生成部121(m)によって自ら認証情報を含む透かしキーG111(m)と同一の透かしキーG121(m)を生成し、電子透かし検証部122(m)がその透かしキーG121(m)を用いて原本画像H(m)から電子透かしを抽出し、改竄の有無を検証して、図示しない記憶制御部に原本画像H(m)を記憶する。また、同様に、画像表示装置130(n)は、透かしキー生成部131(n)によって自ら認証情報を含む透かしキーG111(m)と同一の透かしキーG131(m)を生成し、電子透かし検証部132(n)がその透かしキーG131(m)を用いて原本画像H(m)から電子透かしを抽出し、改竄の有無を検証して、図示しない表示部に原本画像H(m)を表示する。

【0078】したがって、上記第8の実施の形態によれば、画像処理装置から画像管理サーバ、又は、画像管理サーバから画像表示装置へ透かしキーを送る必要が無い場合、画像処理装置のMACアドレスや装置シリアル番号などの装置識別値を画像表示装置にシステム運用開始時に登録しておくだけで、画像表示時には画像管理サーバから画像表示装置に原本画像が送られ、画像表示装置

で表示することができるようになる。例えば、ワークフローとして画像入力装置から画像管理サーバ、画像表示装置へと一連の流れとして送られ表示される場合と、画像表示装置から画像管理サーバに特定画像要求あつて表示される場合のように、互いに原本画像の転送だけ行えば、画像表示装置での表示を行えるため、転送処理の時間の短縮に繋がる。

【0079】なお、上記各実施の形態で説明した透かしキー生成部であれば増加するソフトウェアまたはハードウェアも僅かなもので構成することができる。また、透かしキーを搾取可能な場所が減少することにより、システムとしてセキュリティレベルが向上するという効果が挙げられる。また、上記各実施の形態では、画像管理サーバが一台の場合を想定して説明したが、複数の画像処理装置に対して画像管理サーバも複数ある場合は、システム構成が複雑になるが、画像処理回数を一括管理するサーバをシステム内に置くようにすれば同様に行うことができる。また、それぞれの画像処理装置での画像処理回数が判れば、画像管理サーバが複数であっても上記実施方法が適用できる。画像が送られてきた場合は、画像処理サーバが画像処理回数を問い合わせし、画像処理回数からハッシュ値である画像識別値の生成を行い、その画像識別値から透かしキーを生成して検証を行い、検証が成功すれば原本画像と透かしキーを対で保存するようにすればよい。

【0080】

【発明の効果】以上説明したように本発明の画像処理システムによると、画像ファイルをやりとりする互いの装置でのみ判断できる正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて、電子透かし情報を埋め込んだ画像ファイルから電子透かし情報を抽出できるようにしたため、画像ファイルの改竄の有無を判断することができる効果が得られる。

【0081】したがって、特権ユーザーによる改竄を防止することができるようになり、画像を扱うすべての装置の完全なアクセス権設定作業を低コストで実現できる効果が得られる。また、画像ファイル自体を暗号化する必要がなくなるために、従来のように画像の表示毎に復号化（及び再暗号化）の処理を行わなくてもよくなる。このため、特に、多量の画像を処理するシステムではその処理負荷を小さくでき、画像がシステム内に分散した複数のマシンで利用されるシステムでは、画像の管理が万全となってセキュリティの甘いマシンでの不正を防止できるようになる。

【0082】さらに、検証データの管理に関しての暗号システムがなくても、画像の改竄を検出できるため、暗

号システム自体の管理が高いセキュリティでなくてもよくなる。したがって、本発明では、画像ファイルの改竄を防止し、画像ファイルの改竄を容易に検出し、画像ファイルの処理負荷を小さくした画像処理システムを低コストで提供することができる。

【図面の簡単な説明】

【図1】第1の実施の形態の画像処理システムのネットワーク構成図

【図2】第1の実施の形態の画像処理装置の機能ブロック構成図

【図3】第1の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図4】第1の実施の形態の画像管理サーバの機能ブロック構成図

【図5】第1の実施の形態の画像表示装置の機能ブロック構成図

【図6】第2の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図7】第3の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図8】第3の実施の形態の認証情報生成手段の機能ブロック構成図

【図9】第4の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図10】第5の実施の形態の画像管理サーバの透かしキー生成部の機能ブロック構成図

【図11】第6の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図12】第7の実施の形態の画像処理システムのネットワーク構成図

【図13】第7の実施の形態の画像処理装置の機能ブロック構成図

【図14】第7の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図15】第7の実施の形態の画像管理サーバの機能ブロック構成図

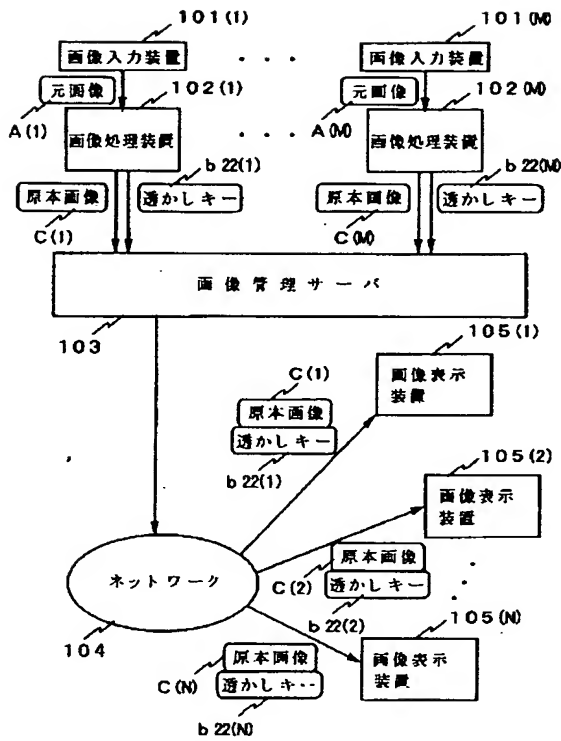
【図16】第7の実施の形態の画像表示装置の機能ブロック構成図

【図17】第8の実施の形態の画像処理システムのネットワーク構成図

【符号の説明】

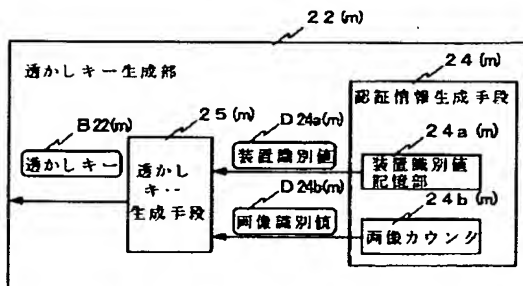
- 101 画像入力装置
- 102 画像処理装置
- 103 画像管理サーバ
- 104 ネットワーク
- 105 画像表示装置

【图 1】



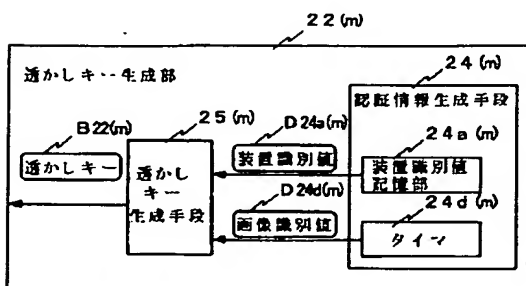
第1の実施の形態の画像処理システムのネットワーク構成図

【図 3】



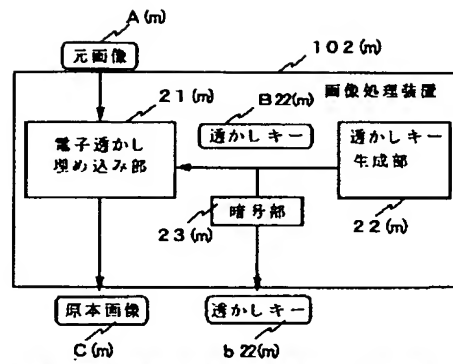
第1の実施の形態の透かしキー生成部の機能ブロック構成図

【図7】



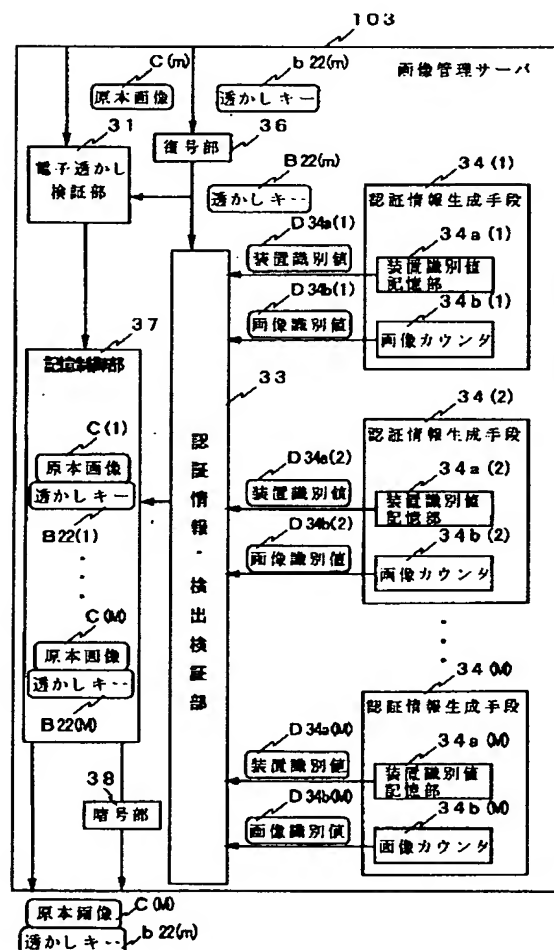
第3の実施の形態の透かしキー生成部の機能ブロック構成図

【図 2】



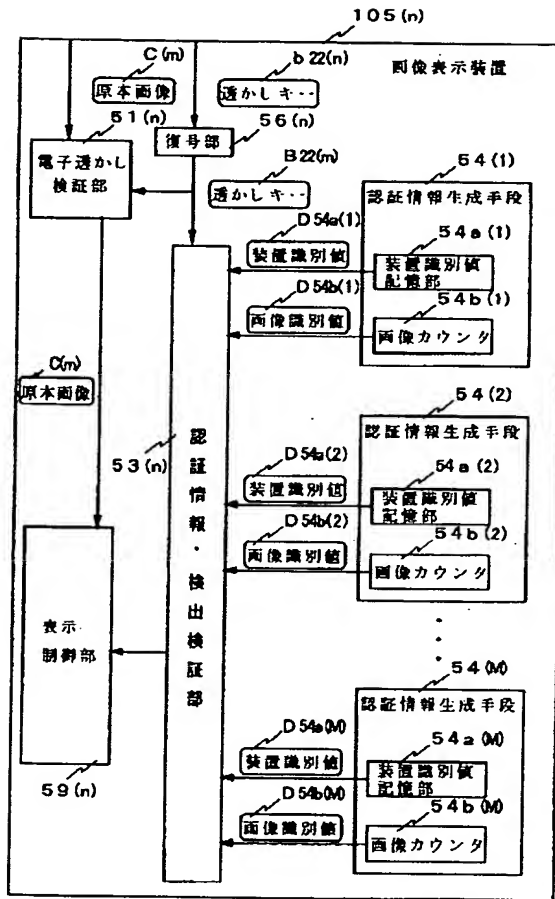
第1の実施の形態の画像処理装置の機能ブロック構成図

【図4】



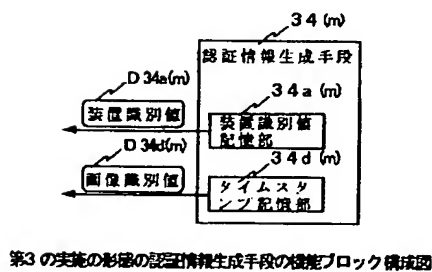
第1の実施形態の画像管理サーバの機能ブロック構成図

【図5】



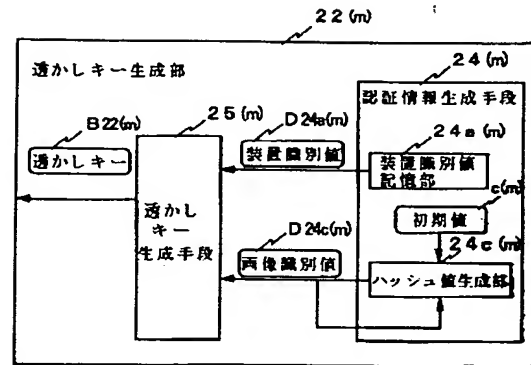
第1の実施の形態の画像表示装置の機能ブロック構成図

【図8】



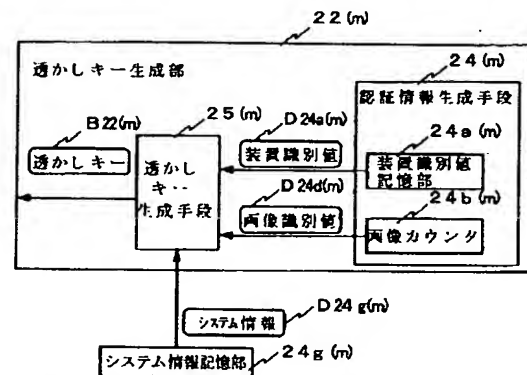
第3の実施の形態の認証情報生成手段の機能ブロック構成図

【図6】



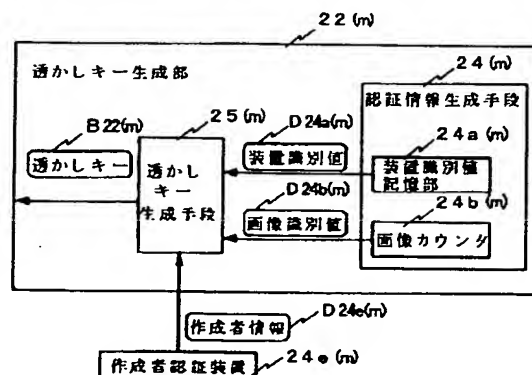
第2の実施の形態の透かしキー生成部の機能ブロック構成図

【図11】



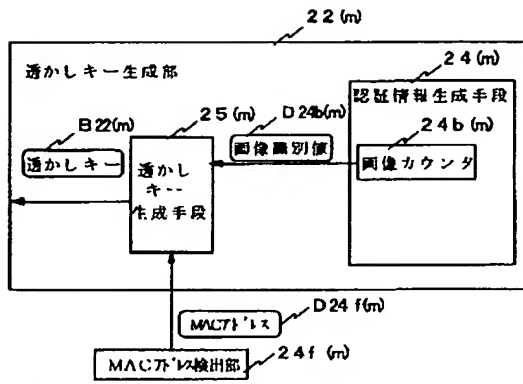
第6の実施の形態の透かしキー生成部の機能ブロック構成図

【図9】



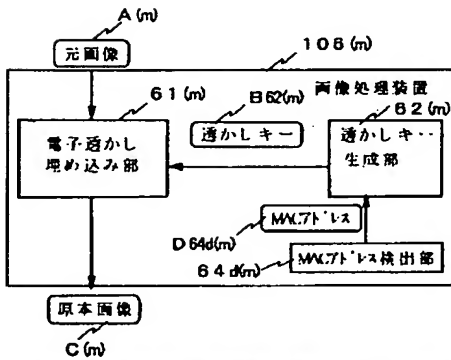
第4の実施の形態の透かしキー生成部の機能ブロック構成図

【図10】



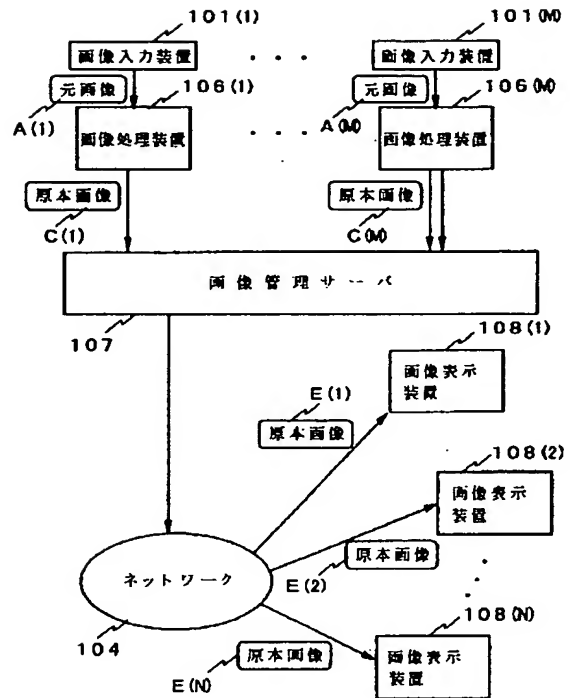
第5の実施の形態の透かしキー生成部の機能ブロック構成図

【図13】



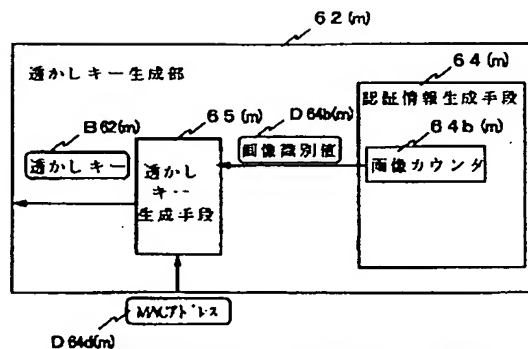
第7の実施の形態の画像処理装置の機能ブロック構成図

【図12】



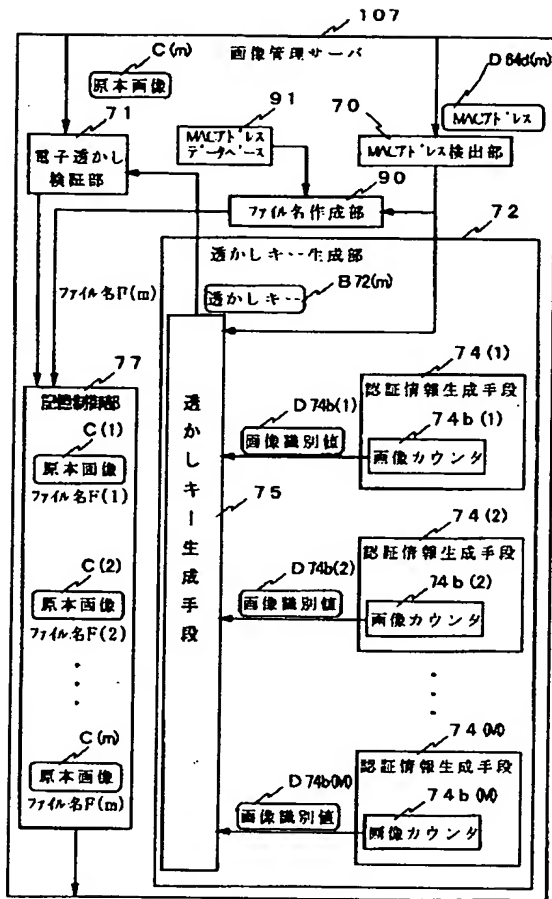
第7の実施の形態の画像処理システムのネットワーク構成図

【図14】



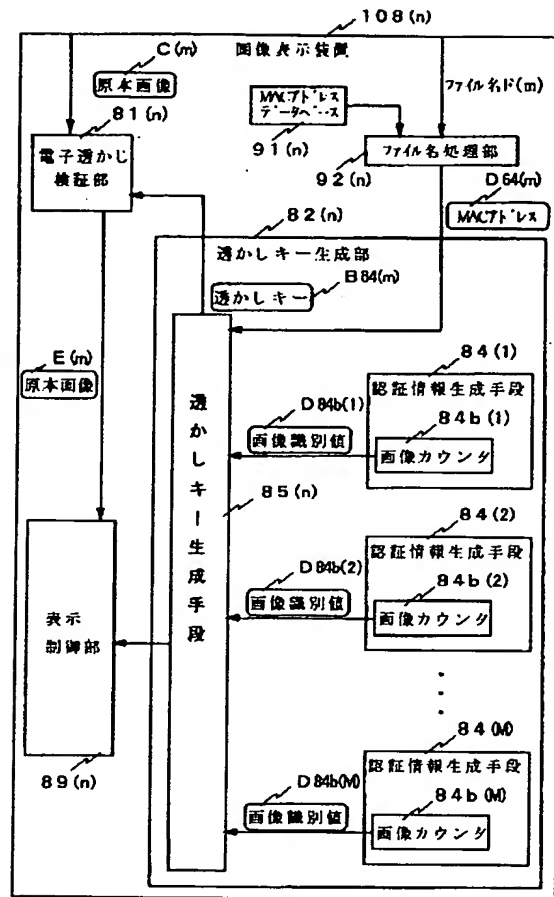
第7の実施の形態の透かしキー生成部の機能ブロック構成図

【図15】



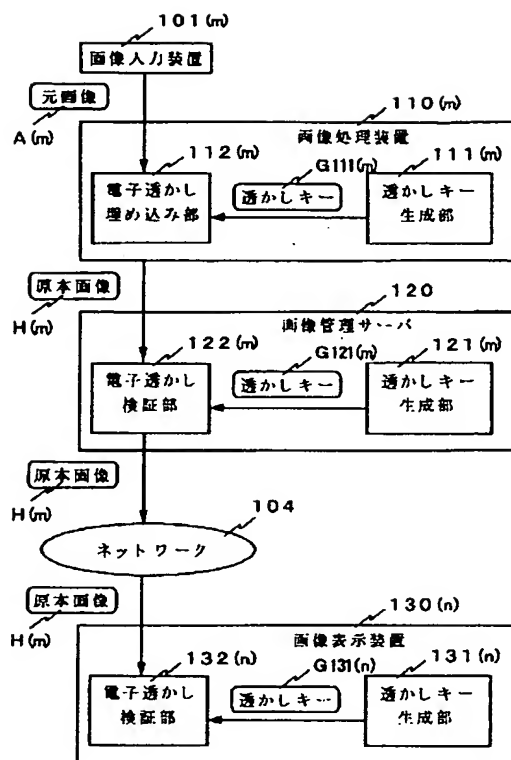
第7の実施の形態の画像管理サーバの機能ブロック構成図

【図16】



第7の実施の形態の画像表示装置の機能ブロック構成図

【図17】



第3の実施の形態の画像処理システムのネットワーク構成図

フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマコード(参考)

9A001

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 CA16
 5B050 BA10 CA08 EA10 EA19 FA02
 GA07 GA08
 5B057 CE08 CG07
 5C076 AA14 BA06
 5J104 AA14 EA10 NA27
 9A001 CC07 HH27 LL03